Krebsz Klaudia

A kibervédelmi törekvések fejlődése és az államok betudhatóságának vizsgálata

Bevezetés

Számos állam igyekszik a kibertérben védelmi mechanizmust kifejleszteni, azonban növekszik azon államok száma, amelyek a kiberteret támadásra szánják. Oroszország az elsők között említhető, de ide soroljuk még, Kínát, Iránt, Észak-Koreát, az USA-t, és az utóbbi időben Izrael, Pakisztán és India képességei is felértékelődtek A megvádolt államok többnyire nem ismerték el, hogy közük lenne a kibertámadásokhoz, és bizonyítékok hiányában, így csak feltételezhető, hogy több kibertámadásban játszottak szerepet.[1] Nagyon nehéz a támadások bizonyíthatósága, mert a kibertérben folyó műveleteknél a legnehezebb bizonyítékokra lelni, leginkább csak az elektronikus nyomok állnak rendelkezésre, de a közvetett bizonyítékokat is számba kell venni, így vizsgálható, hogy melyik országnak fűződött érdeke az akcióhoz. A támadónak azonban az a célja, hogy minden lehetséges nyomot megsemmisítsen, elfedjen, hogy az egyértelmű bizonyítás ne valósulhasson meg és a vádakat tagadni tudja. Kedvelt lépés a proxyművelet, amely annyit tesz, hogy a valódi támadó helyett más cselekszik, amelyhez az agresszor támogatást nyújthat. Ez lehet közvetett is, amikor például egy menekülési útvonalat

1 Berzsenyi Dániel: A kibertér aktuális nemzetközi biztonságpolitikai kihívásai, In: *Incidensmenedzsment. Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára,* Nemzeti közszolgálati Egyetem, 2022. 10. o.

biztosít a végrehajtónak. A proxykapcsolatoknak két fajtája ismert, a belföldi és a külföldi. Az előbbi esetén egy gazdasági társaság/csoport, míg az utóbbi esetében pedig egy másik állam, vagy annak gazdasági szereplőjének/¸csoportjának támogatása valósul meg. A nagy támadások valakinek/valakiknek a számlájára írhatók, azért valamely közösség felel, hiszen egyénileg egy ekkora mértékű károkozás valószínűsíthetően nem tudna megvalósulni. Támadói csoportokat hoztak létre, amelyek közül már elég sokat azonosítottak, és a rendelkezésre álló adatok alapján elmondható, hogy ezeknek a többsége csak úgy tud működni, ha azt egy állam támogatja.[2]

1. Kibertámadások áttekintése és a rájuk adott nemzetközi reakciók

1.1. A NATO elleni korai kibertámadás

A NATO-t először az 1999-ben, Koszovóban végrehajtott bombázását követően érte kibertámadás, szerb, orosz és kínai hackerek által. Ennek oka az volt, hogy amikor jugoszláv tagállamok szakadtak el a szövetségből, az nem ment konfliktusmentesen, és a háborúskodás ezen a területen Koszovóban öltötte a legnagyobb méreteket. A cél homogén nemzetiségű ország létrehozása volt (legalábbis az elnök erre hivatkozott a Hágai Törvényszék előtt is), ezért Szerbia 1998-ban Slobodan Milosevic parancsára etnikai tisztogatásokba kezdett. Falvak ezreit égették fel, tömeggyilkosságokat követtek el, rengeteg ember az otthona elhagyására kényszerült. Ez a szerb lépés a legtöbb nemzetközi szervezetet teljesen megdöbbentette. 1999. február 6-án megkezdték

2 Kralovánszky Kristóf: A kibertér fejlődése= The Evolution of Cyberspace, *Hadmérnök,* 2019/4. 201–202. o.

a béketárgyalásokat Rambouillet-ben, de ez nem járt sikerrel, ezért a NATO 1999. március 24-én Jugoszlávia bombázása kezdett, a hadművelet az Allied Force nevet viseli.[3] Az akciót egyébként az ENSZ Biztonsági Tanácsa nem hagyta jóvá. A bombázások után került sor a szövetség honlapjának megtámadására szerbiai hackerek által. Ebből fakadóan többször is elérhetetlenné vált a weboldal. A támadás a szerb Fekete Kéz (Crna Ruka), az orosz (From Russia With Love) és kínai hackercsoportokhoz volt köthető, amely kormányzati szervereket támadta. A Szövetség ekkor ébredt rá először, hogy egy új típusú kihívással is szembe kell nézniük. Ennek nyomán 2002-ben elindult a szövetség kibervédelmi programja a prágai csúcstalálkozó keretében, és sor került a Számítógépes Incindens Reagáló Központ (NATO Computer Incident Response Capability – NCIRC) létrehozására a NATO rendszerei feltörésének elkerülése céljából. Ettől függetlenül a tagállamok hálózatai és a rendszereinek védelme az ország feladatkörébe tartozott.[4]

1.2. Kibertámadások államok ellen

1.2.1. Az Észtországot ért kibertámadás

2007-ben, Észtország ellen követtek el kibertámadást, melynek kiváltó oka a fővárosban, Tallinban egy szovjet emlékmű eltávolítása volt, amely az ott élő orosz lakosok nemtetszését váltotta

3 Takács Izabella: 78 NAP. A médiapropaganda nyelve az 1999-es évek NATO-bombázásai idején a Magyar Szó című napilap címlapjain, Pécs, 2020. 12–14. o.

4 Kelemen Roland: A kibertámadások nemzetközi jogi olvasata és a NATO általi értelmezése, különös tekintettel a válaszlehetőségekre, In: Farkas Ádám (szerk.): *Az állam katonai védelme az új típusú biztonsági kihívások tükrében*, Nemzeti Közszolgálati Egyetem, Közigazgatási Továbbképzési Intézet, 2019. 46. o.

ki.[5] Az első támadásokra a tüntetéseket követően került sor, központjukban a parlament, kormányhivatalok és a minisztériumok voltak, de támadás érte éppúgy a pénzintézeteket, telefontársaságokat és a médiacégeket is. Egy Arbor Networks nevezetű cég, amely internetes biztonságtechnikával foglalkozik, megfigyelés alatt tartotta a túlterheléses támadásokat, ez idő alatt 128 incidenst észlelt. A megvalósítani kívánt cél kétségtelenül az állam online infrastruktúrájának megbénítása volt, ezzel lehetett elérni a gazdaság és a telekommunikáció összeomlását. Számos intézményben nagy zavart okozott, a bankhálózat átmenetileg megbénult, a telefonhálózat nem működött. Oroszország a nézeteltérés elején még kereskedelmi szankciókkal riogatta Észtországot, azonban ez a virtuális offenzíva még veszélyesebbnek bizonyult a szakértők vélekedése szerint. De hogy mit is jelent számokban a kár? Az észt Hansabank, az ország legnagyobb bankja több mint egymillió dollár veszteséget szenvedett, és ez csupán egyetlen nap leforgása alatt. Ez volt május 10-én, itt érte el tetőpontját a támadás.[6] A körülmények alapján elképzelhetetlen, hogy egy ilyen szinten megszervezett, kifinomult kiberművelet ne egy államnak, hanem attól független magánszemély(ek)nek, hackercsoportoknak a tevékenysége. Az agresszió jellegéből kiindulva az agresszorok kilétének megállapítása csaknem esélytelen. Többeket orosz területen azonosítottak, de bizonyítékok hiányában nem lehetett hitelt érdemlően igazolni, hogy a támadások mögött kormányzati szerverek állnak, de az észtországi eseményeket figyelembe véve csakis Oroszországnak állt érdekében előidézni a támadásokat, természetesen ő mindezt

5 Selján Gábor – Selján Péter: Kiberbiztonsági kitekintés, *Nemzet és Biztonság*. 2021/1. 30. o.

6 Bányász Péter – Orbók Ákos. A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében, *Hadtudomány*, 2013/23. 191–192. o.

tagadta.[7] 2009-ben Konsztantyin Goloszkokov, a NÁSI, vagyis egy ifjúsági mozgalom vezetője bevallotta, hogy a cselekményeket ők okozták, és ők ezt egyáltalán nem támadásnak vélték, épp ellenkezőleg. Szerintük egy ez ellenoffenzíva volt a szerintük illegálisan eltávolított emlékmű miatt. Goloszkokov állítása alapján a támadás a saját döntésük volt és a kormánynak ehhez semmi köze, így az ismertté vált álláspont szerint a cselekmények olyan orosz hackerek műve, akik rosszallták a szovjet emlékmű likvidálását.[8]

1.2.2. A Grúziát ért kibertámadás

2008-ban Oroszország és Grúzia közötti fegyveres összeütközés során, sőt azt megelőzően is Grúziában egyes weboldalak, szerverek egy időre megszűntek működni, a kapcsolattartás akadályoztatva volt. Ennek előzménye, hogy a grúz elnök a grúz-oszét és a grúz-abház ellentétek rendezését katonai úton kívánta véghez vinni, de Oroszország ezt nem hagyta szó nélkül. Grúzia öt nap után feladta a harcot, és fegyverszünetet kért. Az orosz ellenválasz nemcsak fizikai összecsapásokban mutatkozott meg, hanem Moszkva a kiberképességeit is megcsillogtatta. A legmarkánsabb támadások Grúzia kormányzati portáljait tették működésképtelenné, valamint ezeken tartalommódosításokat hajtottak végre. Ez a defacement, másnéven honlaprongálásos támadás. Többek között az elnökből, Mihail Szakasvili-ből próbáltak gúnyt űzni azzal, hogy fotójára Hitler-bajuszt rajzoltak, ezen kívül megjelentek olyan képek is, ahol az elnököt Hitler tipikus pózaiban jelenítették meg. Ezen tevékenységekért Oroszországot vádolták, de ő tagadta, hogy a kormánynak köze lenne a cselekményekhez.

---

7 Szentgáli Gergely: A NATO kibervédelmi politikájának fejlődése, *Nemzet és Biztonság*, 2013/3–4. 78. o.

8 Bányász – Orbók: i. m. 192. o.

A kormány szóvivője azt azonban nem zárta ki, hogy ugyan állami támogatás nélkül, de előidézhették orosz polgárok is, akik így próbáltak véleményt formálni a grúz inváziójáról. Grúzia nem rendelkezik olyan fejlett kiberinfrastruktúrával, mint mondjuk Észtország, ezért az ellenük elkövetett kibertámadás kevésbé értékelhető nagymértékű károkozásnak.[9]

1.3. A kibervédelem fejlődési lépcsőfokai

A 2007-es észt, és az azt követő 2008-as grúz támadások következtében szükséges volt a kibervédelmi fejlesztések továbbgondolása, ugyanis itt mutatkozott meg legelőször, hogy milyen volumenű támadások hajthatók végre kibertéren keresztül, amelyek már egyértelműen visszahatnak a hagyományos térre is (lásd például a banki szolgáltatások leállása). 2007-ben került sor a brüsszeli védelmi minisztériumi csúcstalálkozóra, és itt fogalmazódott meg az igény egy összehangolt kibervédelmi stratégai kidolgozására. Ebből a célból fogadtak el 2008 elején Bukarestben egy új Kibervédelmi Irányelvet, amely a nemzetek eljárásának egységesítését szorgalmazta, ugyanis a NATO-nak és a „nemzeteknek is meg kell védeniük a kulcsfontosságú informatikai rendszereiket, meg kell osztaniuk a legjobb gyakorlatokat és biztosítaniuk kell a szövetséges nemzetek számára, hogy kérésre segítséget nyújthassanak a kibertámadások elhárításához."[10] A védelmi kapacitások erősítésére pár hónappal később, májusban került sor a Kooperatív Kibervédelmi Kiválósági Központ (Cooperative Cyber Defence Centre of Excellence, CCDCOE)

9 Berki Gábor: Kiberháborúk, kiberkonfliktusok, In: *Műhelymunkák,* Geopolitikai Tanács Közhasznú Alapítvány, Budapest, 2016. 266–267. o.

10 *Bucharest Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic*, Council in Bucharest, 2008.

felállítására Tallinnben, amelynek Magyarország 2010 óta tagja.[11] Ennek a lényege, hogy a szövetség tagállamai a kibervédelmi tapasztalataik megosztásával segítsék egymás fejlődését. A szervezet projektjei között kibervédelmi gyakorlatok és konferenciák szerepelnek, ahol a jelenlévőknek lehetőségük adódik gyakorolni és megtanulni, hogy mégis milyen technikával lehet kivédeni egy igazi kibertámadást. Az Észak- atlanti Tanács még az alapítás évének őszén jogilag is nemzetközi katonai szervezetnek minősítette a Központot.[12] Emellett kialakítottak egy hatóságot (Cyber Defence Management Authority – CDMA) a kibervédelmi problémák kezelésére. Ez a Cyber Defence Management Board irányítása alatt tevékenykedik (NATO Kibervédelmi Irányító Testület), amelynek feladata a centralizált kibervédelem irányítása, a tagállamok támadásra reagálása, ezeken kívül a nemzeti kibervédelem kialakításában való segítségnyújtás. A Számítógépes Incidens Reagáló Központ alatt működik a Rapid Reaction Team (gyorsreagáló csoport), amely a nemzeteket segíti a támadásokkal szemben. Nemzeti szinten létesítésre került a Computer Emergency Response Team (CERT, Számítástechnikai Sürgősségi Reagáló Egység).[13] 2009-ben az USA felállította a kiberhadviselésért felelős parancsnokságot (USCYBERCOM). 2013-ban a Nemzeti Hírszerzési Igazgató, James Clapper a legsúlyosabb fenyegetésnek a virtuális fenyegetést jelölte meg, amely így háttérbe szorította a terrorizmust, pedig 2001. szeptember 11. óta az efféle akciók jelentették a legnagyobb veszélyt.[14]

11 Kelemen: i. m. (2019) 46–47. o.

12 Tóth Tamás: A NATO Kibervédelmi Kiválósági Központ bemutatása. *Nemzetbiztonsági Szemle*, 2018/4. 51–53. o.

13 Kelemen: i. m. (2019) 47. o.

14 Selján: i. m. 30. o.

2010-ben a lisszaboni csúcson került elfogadásra a szövetség új Stratégiai Koncepciója, amelynek sarkalatos részét adták a kibertevékenységek.[15] Leszögezte, hogy a kibertámadások egyre gyakoribbá, szervezettebbé váltak, illetve a kormányok, vállalkozások, gazdaságok és potenciálisan a közlekedési és ellátási hálózatok, valamint más kritikus infrastruktúrák számára is egyre nagyobb károkat okoznak. Elérhetik azt a küszöböt, ami már a nemzeti és euroatlanti prosperitást, biztonságot és stabilitást veszélyezteti.[16] Célként szerepelt a képességek továbbfejlesztése és a NATO-szervezetek centralizált kibervédelmének megvalósítása. 2011 júniusában Brüsszelben tartották a védelmi miniszterek találkozóját, ahol átalakították a Kibervédelmi Irányelvet, és elfogadásra került a Cselekvési Terv is, amely bevezette az újításokat a gyakorlatba. A 2012-es chicagói csúcson ismételten számottevő jelentőségű volt a kibervédelem. Ezen a találkozón megfogalmazásra került, hogy a támadások száma egyre csak nőni fog, egyre kifinomultabbakká és összetettebbekké válnak. Ugyanebben az évben Tallinnben került megrendezésre a CyCon – konferencia is, ahol elhangzott, hogy a szövetség az elosztott felelősség elvét alkalmazza a kiberbiztonságban, ehhez el kell egymástól választani a nemzeti és a NATO kiberbiztonsági követelményeit. „Minimum követelményeket kell meghatározni azon nemzeti infrastruktúrák kiberbiztonságára, amelyek NATO-műveleteket is támogatnak annak érdekében, hogy ne legyen biztonsági rés a NATO és a nemzeti infrastruktúrák védelmi szintje között."[17] 2018-ban a brüsszeli csúcstalálkozón rögzítették az Eu és NATO együttműködését a közös biztonsági fenyegetésekkel szemben, melynek középpontjában többek között a kiberbiztonság, a hibrid

15 Kelemen: i. m. (2019) 47. o.
16 Kelemen: i. m. (2019) 47. o.
17 Kelemen: i. m. (2019) 48. o.

fenyegetések állnak.[18] A 2022-es madridi csúcson megfogalmazásra került, hogy Oroszország a legnagyobb fenyegetést jelenti közvetlen katonai szempontból, ezért fontos, hogy a tagállamok védelmi képességeiket erősítsék.[19]

1.4. A kiberháborúra alkalmazandó nemzetközi jog Tallinni Kézikönyve, mint egy szakértői iránymutatás – Az első szakértői vélemény vázlatos bemutatása

2013-ban került sor A Tallinni Kézikönyv a kiberhadviselésre alkalmazandó nemzetközi jogról (Tallinn Manual on the International Law Applicable to Cyber Warfare, röviden: Tallinni Kézikönyv) című szakértői dokumentum kiadására, amely értelmezni és rendszerezni próbálja az kiberhadviselésre vonatkozó nemzetközi jog kereteit.[20] A kidolgozás igazgatója Michael N. Schmitt, koordinátora pedig Dr. Eneken Tikk. A Tallinni Kézikönyv foglalkozott elsőnek a téma átfogó vizsgálatával, habár nem kötelező erejű, csupán egy iránymutatás, javaslat, amelyet az államok átvehetnek a kibertérrel kapcsolatos nemzeti jogi értelmezésükbe.[21] A kézikönyv gyakorlatilag az Államfelelősségi Tervezetben kialakított állami betudhatóságot vetíti ki a kibertérben megvalósított cselekedetekért, bizonyos módosításokkal, kiegészítésekkel.

---

18 Európai Tanács: *NATO-csúcstalálkozó, Brüsszel, 2018. július 11–12., 2018. július 11–12,* (https://www.consilium.europa.eu/hu/meetings/international-summit/2018/07/11-12/).

19 Csiki Varga Tamás – Tálas Péter: Megerősített elrettentés és védelem – a NATO új stratégiai koncepciójának és madridi csúcstalálkozójának értékelése, *Stratégiai Védelmi Kutatóintézet Elemzések*, 2022/8. 1. o.

20 Michael N. Schmitt (Ed.): *Tallin Manual ont he international law applicable to cyber warfare*. Cambridge University Press, Cambridge, 2013.

21 Gyebrovszki Tamás: Stuxnet-mint az első alkalmazott kiberfegyver – A Tallinni Kézikönyv szabályrendszere szempontjából, *Hadmérnök*, 2014/1. 166. o.

(1) *Az államok jogi felelőssége*:
Az államot nemzetközi jogi felelősség terheli a neki felróható nemzetközi jogot sértő kiberműveletekért vagy bizonyos esetekben mulasztásokért, így például az ENSZ Alapokmányának, vagy a békeidőre szóló szabályok megsértése is ide tartozik. A kár okozása nem feltétlenül szükséges a kiberművelet nemzetközileg jogellenes minősítéséhez. Ha mégis van ilyen szabály, a kár szükségképpen kell az államfelelősség megállapításához. Az állami szerveknek még az ultra vires tevékenységei is megalapozzák az állam felelősségét, ha általuk nemzetközi jogsértés következik be, de ez akkor is így van, ha a személyek, entitások kormányzati hatalmat gyakorolnak. Nem állami szereplő magatartása is alapul szolgálhat az államfelelősség kialakulásához. Az a kiberművelet, amely olyan személyhez, csoportokhoz köthető, akik az állam utasítása, irányítása vagy ellenőrzése alatt tevékenykednek, állami cselekménynek tekintendő. Az elkövetés helye irreleváns az államfelelősség megállapításához, ha egy állam más államok számítógépeit felhasználva valósít meg kibertevékenységet, a felelősség a számítógépet felhasználó államot terheli. Szintén állami cselekménynek minősülnek azok a magatartások, amelyeket az állam sajátjaként elismer.

(2) *A kormányzati kiberinfrastrukúrából indított kiberműveletek*:
Annak ténye, hogy kiberműveletet indítottak, vagy az kormányzati infrastruktúrából származik, önmagában nem elég bizonyíték arra, hogy a művelet az államnak tulajdonítható, csupán az állam érintettségét igazolja.

(3) *Az államon keresztül indított kiberműveletek*:
Szintén nem elég bizonyíték az államhoz köthetőséghez, ha egy cselekményt egy államban található kiberinfrastruktúrán keresztül irányítottak át. Ez akkor valósul meg, ha az egyik állam kiberinfrastruktúrájában indul meg a művelet, de áthalad egy másik állam kiberinfrastruktúráján. Az utóbbi államnál nem feltételezhető, hogy részt vesz a műveletben. Azonban ha tisztában van

a tranzittal, és nem tesz észszerű intézkedéseket a megakadályozására, a felelőssége fennáll.

A szakértők úgy vélekedtek, hogy az ellenintézkedéseknek szükségesnek és arányosnak kell lenniük, továbbá csak akkor jogszerű, ha a másik állam cselekménye jogsértő, előtte azonban fel kell szólítania a jogsértő államot a jogsértés befejezésére. Ha a jogellenesség megszűnt, a sértett állam nem tarthatja fent ellenintézkedéseit, illetve nem is kezdeményezhet utóbb.[22]

1.5. Hibrid hadviselés Krímen és Ukrajnában a Geraszimov – cikk alapján

2013-ban Valerij Vasziljevics Geraszimov orosz vezérkari főnök egy új hadviselési módot, a hibrid hadviselést fogalmazta meg, amelyet egy újabb generációnak tekint. Eszerint hibrid háború a diplomáciai eszközök vegyítésével valósul meg. A direkt katonai beavatkozás helyett, vagy azzal párhuzamosan egyéb eszközök használata is megjelenik, különösen a kritikus infrastruktúra a fő célpont. Geraszimov szerint a hadviselés már nem a régi szabályok szerint folyik. Előnyben részesítik az indirekt erő bevetését (félkatonai, civil felkelők), és az információs tér adta lehetőségeket. Támogatja a tömeges bevetést, különleges erők, robotizált fegyverek (pl. drónok) használatát. Surkov/Dubovitksy, Peter Pomerantsev ezt az új hadviselést nem lineárisként írta le, majd 2014 májusában az International Herald Tribune is ezt a szókapcsolatot használta. A holland tábornok, Frank van Kappen az orosz csapásokat hibrid háborúként értékelte. 2014. július 3-án fogadta el a NATO ezt a kifejezést. A cél az ellenség befolyásolása és belső bomlasztása. A háborúban a hátországnak is nagy szerepe van. Rácz András a hibrid hadviselést 4 fázisra osztja,

22 Michael N. Schmitt (Ed.): *Tallinn manual on the international law applicable to cyber warfare,* Cambridge University Press, Cambridge, 2013. 29–36.

ezek a következők: előkészítési, politikai előkészítési, műveleti előkészítési, támadási és az elért siker stratégiai kihasználási fázisok.[23] A hadviselés megfigyelhető a Krímen és Ukrajnában is, amelyről kicsit lejjebb ejtek szót. A cikk tartalmát Geraszimov átültette a 2014-ben megjelent doktrínájában is, amely egy nem hivatalosan elfogadott dokumentum. Szintén feltűnik a tartalmában, hogy az új hadviseléshez szükséges más eszközök bevetése is a hagyományos fegyveres csapatokkal együtt. Geraszimov tanulmányában említi az Arab Tavaszt, amelynek pusztításait a valódi háborúhoz hasonlítja. Megfogalmazta, hogy a hagyományos módszereken kívüliek nagyobb hangsúlyt kaptak, azok nagyban hozzájárultak a politikai és stratégiai célok megvalósításában. Szerinte a kiberhadviselés segíti az ellenfél harci képességeinek mérséklését, és fontosnak tartja a támadások elleni védekezési képességet. Ez az anyag egyszer sem tesz említést a hibrid háborúra vagy a hadviselésre, de a doktrína kifejezés sincs nevesítve.[24] A tanulmány készítője így vélekedik a munkáról: „Geraszimov munkáját inkább egy hidegháborús nyelvezetre emlékeztető, a hadtudomány művelőinek szánt, kutatandó célokat, feladatokat, elméleti fejtegetéseket tartalmazó cikként lehet meghatározni és nem egy ún. „hibrid háborút" meghirdető katonai doktrínaként." [25] Gudrun Perrson is úgy vélekedett, hogy az Arab Tavaszhoz hasonlatos háborúk fenyegethetik Oroszországot, főleg azért, mert az orosz hadtudomány az amerikainak a közelébe sem érhet. Galeotti szerint a doktrínában foglaltakat aszopikusnak jellemezte, mert ugyan Geraszimov arról írt, hogy

23 Rácz András: Russia's Hybrid War in Ukraine Breaking the Enemy's Ability to Resist. *Finnish Institute of International Affairs Report 43,* 2015. 36–41. o.

24 Tomolya János: Az úgynevezett „Geraszimov-cikk" margójára, *Hadtudomány*, 2018/3–4. 80–81. o.

25 Tomolya: i. m. 85–86. o.

az új hadviselési mód fenyegető Oroszországra nézve, és meg kell tőle védeni az országot, valójában arra gondolt, hogy Oroszországnak kell használnia ezt a hadviselést. Tehát ugyan az írásban védekezésről van szó, de azt támadásnak kell értelmezni.[26]

A negyedik generációs hibriditást alkalmazva a Krím- félsziget annektálásának sikere érdekében 2013-tól végeztek az oroszok kibertevékenységet, ami 2015-ben több órás áramkimaradáshoz is vezetett. Ez a támadás olyan kifinomult és rendkívül összehangolt volt, hogy arra enged következtetni, az akciók mögött csak egy állam állhatott. 2014-ben pedig az oroszok Ukrajnát támadták meg, és nagy területeket foglaltak el a keleti országrészen.[27] A támadás három szakaszból állt, és minden szakaszon belül három fázis valósult meg. Makhmut Garajev tábornok álláspontja szerint a technológiai fejlődésnek hála, a hadviselés megváltozott. Az új számítógépek, elektronikus eszközökkel nagyon hamar információhoz lehet jutni, a reakcióidő pedig ezzel együtt jelentősen lecsökken. A kiberhadműveletek képesek zavart okozni az ellenség kapcsolattartásában, radarok, hadműveleti eszközök működésében. További előnyt jelent, hogy így lehetőség van áttérni egy látens, előre be nem jelentett háborúra. Vladimir Slipchenko tábornok ezt a gondolatmenetet vette át, továbbfejlesztve. Szerinte a jövő csatái „érintkezés nélküli" összecsapások lesznek, az ostrom a levegőből és a világűrből érkezik. Domináns célpontok a katonai, politikai és gazdasági érdekeltségű infrastruktúrák, melyet hagyományos fegyveres támadás nélkül kívánnak megvalósítani. A Svéd Védelmi Kutatási Ügynökség (Swedish Defence Research Agency, FOI) szakértői szerint az orosz hadművelet nagyrészt a régi volt, elnézve a katonai képességeket, dezinformációs eszközöket, azonban a katonai

26 Rácz: i. m. 15. o.
27 Selján: i. m. 35. o.

és informatikai eszközöket hatékonyan összehangolták.[28] A 2014-es walesi csúcstalálkozó eredeti céljai között a transzatlanti kapcsolatok megújítása, a szövetség bővítése és a képességek fejlesztése szerepelt,[29] azonban az ukrán helyzet felhívta a figyelmet a kollektív védelem fontosságára, és így váratlanul került napirendi tűzésre a válság megoldása.[30] A támadások irányulhatnak választások ellen is, ez történt 2015-ben, amikor Ukrajna ellen követtek el virtuális támadásokat a választások eredményének befolyásolása céljából. A tevékenységekkel Oroszországot vádolták, de az állam nem ismerte el felelősségét. A szakértők véleménye az elkövetőkről ebben a kérdésben eltérő, egyesek a Fancy Bear nevű hackercsoporthoz kötötték az akciókat.[31] A Kibervédelmi Felajánlás (Cyber Defence Pledge) elfogadására 2016-ban, a varsói védelmi miniszteri találkozón került sor. Ebben került elismerésre a tagállamok állam- és kormányfői által a biztonsági fenyegetések új arca, a kiberfenyegetések, amelytől a nemzeteket meg kell védeni. Így kötelezettségüket megerősítették, és a tagállamok vállalták, hogy a tőlük elvárható legmagasabb színvonalú védelmet nyújtják, és együttműködnek a tagországokkal.[32] A félszigeten történtek hatására ismerte el a NATO a kiberteret a szárazföld, tenger, levegő, világűr mellett újabb dimenziónak. Ezáltal, ha egy esetleges támadás olyan mértéket ölt, mint egy fizikai támadás, ellentámadás indítható, de nem csak a kibertérben. Egy ilyen eset volt, amikor az USA felkutatta

28 Rácz: i. m. 34–36., 51. o.

29 Szenes Zoltán: Új bor a régi palackban?, A walesi NATO–csúcs, *Hadtudomány*, 2014/3–4. 6. o.

30 Kelemen: i. m. (2019) 48. o.

31 Berzsenyi Dániel: A kibertér aktuális nemzetközi biztonságpolitikai kihívásai, In: *Incidensmenedzsment. Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára,* Nemzeti közszolgálati Egyetem, 2022. 11–12. o.

32 Kelemen: i. m. (2019) 49. o.

és megsemmisítette az Iszlám Állam hackereit, habár ez nem a NATO-hoz köthető. Az új hadszíntér megjelenésének okai között említhetjük, hogy az Egyesült Államok szerint a riválisaival szemben sokkal erősebb és intenzívebb védelemre van szükség, ehhez ő a segítségét nyújtotta. Az Egyesült Királyság közölte, hogy nem hagyja szó nélkül az ország kritikus infrastruktúrái ellen más kormány által végrehajtott támadást. Németország és Franciaország is támogatták a harcias virtuális képességek. Ezen államok részvételével a szövetségen belül egy belső kiberbiztonsági közösség jött lére, melynek a legmeghatározóbb alakja az USA volt. A kiberbiztonság megoldására összehangolt metódus nem alakult ki, az első, USA- hoz köthető ilyen módszer 2003-ból ismert, majd ezt követően a többi meghatározó állam is kialakította saját stratégiáit. Franciaország az egyetlen olyan állam a négyes közösségből, aki a legnagyobb veszélyt a nem állami szereplőkben (mint például a kiberterroristákban) látta, a többi hatalom továbbra is az államoktól tart. A szövetség az oroszok keltette problémát úgy kívánta megoldani, hogy ne vezessen a kapcsolatok megszakadásához Oroszországgal.[33] Az orosz-ukrán konfliktus hatására az Európai Uniót foglalkoztatni kezdte a dezinformációs tevékenységek blokkolása, amelyek a hibrid háborúk részét képezik, így 2015-ben létrejött az East StratCom Task Force nevezetű munkacsoport, amely arra irányult, hogy a külső szereplők általi félretájékoztatás mielőbb kitudódjon. Erre 2018-ban kidolgoztak egy cselekvési tervet is, amely úgy rendelkezik, hogy ezekkel szemben a tagállamoknak és az unió intézményeinek osztottan kell reagálniuk. Tartalmazza továbbá, hogy a kérdésben feladattal érintett szervek megerősítése szükséges, és egy riasztási rendszert is ki kell alakítani, amely majd a valós időben jelzi a problémát. A platformok felelőssége is megjelenik. Egy újabb előrelépés volt azonban a 2019-ben felállított Rapid

33 Selján: i. m. (2021) 25. o.

Alert System, amely egyszerűbb tájékoztatást és egységesebb fellépést biztosít a tagállamoknak és az uniós intézményeknek a dezinformáció kezelésére, ezáltal létrehoztak egy hálózatot a koordinálás és a tapasztalatok megosztása céljából, amelyhez a 27 tagállam kapcsolódik. A koronavírus járvány infodémiát (információs fertőzést) okozott, és az Unió felismerte, hogy meg kell egymástól különböztetni a hamis (jogellenes) és a félrevezető (káros) tartalmakat. A félrevezető tartalmaknál akkor merül fel félretájékoztatás, „ha megtévesztés, közérdeknek való károkozás vagy gazdasági károkozás szándékával tették közzé."[34] Azt, hogy melyik tartalom melyik csoportba sorolható, az adott tagállam ítéli meg.[35]

1.6. Tallinn Manual 2.0

A *Tallinni Kézikönyv 2.0 – A kiberműveletekre alkalmazandó nemzetközi jogról* című szakértői vélemény, ahogyan a nevében is szerepel, a kiberműveletekkel foglalkozik, és erre vonatkozóan betudhatósági eseteket állapít meg.[36] Gyakorlatilag a korábbi ajánlásokat fejleszti tovább és egészíti ki, kötelező erővel ezen dokumentum sem rendelkezi. Jelen fejezetben részletesen kifejtem a kézikönyvben szereplő betudhatósági eseteket, és röviden összevetem a 2001-es Államfelelősségi Tervezettel.

(1) *Nemzetközileg jogellenes kiberjogi cselekmények:*

A kézikönyv úgy rendelkezik, hogy a nemzetközi jogot sértő cselekmény, vagy mulasztás elkövetése tekintetében nemzetközi

34 Kelemen Roland: Radikalizálás, dezinformálás és tömegpszichózis modern köntösben: a hibrid konfliktus kibertérben, *Jog Állam Politika,* 2021/3. 79. o.

35 Kelemen: i. m. (2021) 79. o.

36 Michael N. Schmitt (Ed.): *Tallinn manual 2.0 on the international law applicable to cyber operations*, Cambridge University Press, 2017.

jogi felelősség terheli az államot, amennyiben a kibercselekmény az államnak tulajdonítható.[37]

Ez az Államfelelősségi Tervezetben is megtalálható, mint betudhatósági eset.[38]

(2) *Állami szervek által megalapozott államfelelősség:*
A Tallin 2.0. szerint az állam szervei, személyek vagy szervezetek kormányzati hatalom elemeinek gyakorlása során az állam által ténylegesen teljes függőségben végrehajtott kiberműveletek állami tevékenységnek számítanak. Itt figyelemmel kell lenni arra, hogy az állami tulajdonban lévő szervek nem feltétlenül minősülnek állami szerveknek. Ha egy szerv a rábízott hatásköröket túllépve nemzetközi kötelezettséget sért, az állam felelőssé tehető akkor is, ha az állam utasításait megsértve cselekszik. Ez akkor is így van, ha személyek vagy egy szervezet állami felhatalmazás alapján állami jogkörök egyes elemeit gyakorolják, és az állam nevében járnak el. Magánszemélyek esetében hivatalos, látszólag hivatalos, vagy a hatalom színe alatti cselekményei, mulasztásai államnak való felróhatóságot eredményeznek. Előfordulhat, hogy az állam nem képes egyes feladatokat ellátni, ezért ezeket magán, vagy önkéntes szervezetekre bízhatja, de ettől a felelősség ugyanúgy az államot terheli.[39]

A Tervezetben is szerepel, hogy az állami szervek, valamint az olyan személyek, szervek magatartása, amelyek közhatalmi elemet gyakorolnak, de nem állami szervek, állami tevékenységnek számítanak.[40]

(3) *Más állam átengedett szerve*:
Ha egy állam valamely szervét más állam rendelkezésére bocsátja, kormányzati funkciók gyakorlása során a fogadó államnak

37 Schmitt: i. m. (2017) 84–87.
38 *Draft articles on the responsibility of international organizations.*
39 Schmitt: i. m. (2017) 87–92.
40 *Draft articles on the responsibility of international organizations.*

lesz betudható, amennyiben az irányítást és ellenőrzést kizárólag ezen állam gyakorolja, valamint a műveleteket az állam nevében, az ő céljai megvalósítása végett végzi. Ezen szerv ultra vires tevékenysége esetében is szintén ez a helyzet áll fenn.[41]

Az Államfelelősségi Tervezet nemcsak átengedett szervekről, hanem személyekről is rendelkezik,[42] ezáltal a betudhatóság e tekintetben bővebb, mint a kézikönyvnél, ugyanis ott csak átengedett szerveket említ. Ezen kívül ez a pont is megfeleltethető a 2001-es ajánlásnak.

(4) *Nem állami szereplők tevékenysége:*
Ebben az esetben az államot akkor terheli felelősség, ha az ő utasításai szerint, irányítása vagy ellenőrzése alatt végzik vagy az állam a műveleteket elismeri és sajátjaként fogadja el.[43]

A kézikönyv itt említi az egyéni hackereket, informális csoportokat (pl. Anonymous), bűnszervezeteket, kiberterroristákat és lázadókat. Leggyakrabban a nem állami szereplő az állam segítője, és ultra vires cselekményeik általában nem tulajdoníthatók az államnak, csak ha a művelet lényeges részét jelenti annak, amely felett az állam hatalmat gyakorol.[44]

A Tervezetben szintén szerepelnek azon személyek tevékenységei, akik állami irányítás, ellenőrzés és utasítás alatt állnak.[45] Ami jelentős különbség a két dokumentum között ezen pont alapján, hogy a 2001-es külön pontban rendezi az államfelelősség azon esetkörét, amikor az állam sajátjaként ismer el egy tevékenységet, és nem korlátozza az állam sajátjaként való elismerést csak a nem állami szereplők esetére, a kézikönyv viszont erre szűkíti a kört.

41 Schmitt: i. m. (2017) 93–94.
42 *Draft articles on the responsibility of international organizations.*
43 Schmitt: i. m. (2017) 94.
44 Schmitt: i. m. (2017) 95.
45 *Draft articles on the responsibility of international organizations.*

(5) *Más államok kiberműveleteivel kapcsolatos felelősség* esetén a felelősség az államot terheli, ha

a) nemzetközi jogot sértő cselekmény elkövetésében egy másik államnak segítséget vagy támogatást nyújt, ha az állam a jogellenesség tudatában nyújt segítséget vagy támogatást, és a cselekmény nemzetközileg jogellenes lenne, ha azt az állam követné el;

b) egy másik állam az irányítása és ellenőrzése alatt elkövetett nemzetközileg jogellenes cselekménye, ha az irányítás és ellenőrzés a jogellenes cselekmény körülményeinek ismeretében történik, és a cselekmény nemzetközileg jogellenes lenne, ha azt ő követné el; vagy

c) nemzetközileg jogellenes cselekmény elkövetésére egy másik államot kényszerít.[46]

Ugyan ezt a tervezet nem egy cikk alatt tárgyalja, de mindhárom esetkör megtalálható benne.

(6) *A kiberműveletek jogellenességét kizáró körülmények*:

A Tallinni Kézikönyv hat jogellenességet kizáró körülményt ismer el, ezek a beleegyezés; az önvédelem, az ellenintézkedések, a végveszély, a vis maior vagy a szükséghelyzet.[47]

Ugyanezeket sorolja fel az Államfelelősségi Tervezet is, valamint mindkettő tartalmazza, hogy a kötelező normák (államok által elfogadott és elismert, amelytől nem lehet eltérni) megsértése nem zárja ki a cselekmény jogellenességét.[48]

Az államok részéről szükséges egy előzetes döntés azzal kapcsolatosan, hogy a tevékenység a másik államnak tulajdonítható. Egyes esetekben rövid idő áll csak rendelkezésére arra, hogy felmérje a releváns információkat a kibertérben. Ekkor az észszerűséget kell szem előtt tartani, amely minden esetben kontextusfüggő.

46 Schmitt: i. m. (2017) 100.

47 Schmitt: i. m. (2017) 104.

48 *Draft articles on the responsibility of international organizations.*

A felelősségre vonás függ a kiberművelet hatóerejétől, valamint a válaszlépés nagyságától, amelynek arányban kell állnia a kibertevékenységgel. Ha a válaszlépést alkalmazó állam téves bizonyítékokra alapozza azt, felelős a tetteiért. Ahogy a kézikönyv elődjében is szerepel, az elkövetés helye többségében nem számít a felelősségre vonásnál, hiszen államterületen kívülről is képesek az államok kiberműveletet kezdeményezni, ha egy nem állami szereplő egy másik állam utasításainak tesz eleget, ahol természetesen az utasítás helye szerinti állam tehető felelőssé, nem pedig az, ahonnan a művelet származik, ő ugyanis maximum a korrekciós műveletek elmulasztásáért felel. Így kibertevékenység folytatható saját államterületről, más állam területéről, tengerről, légtérből vagy a világűrből. Minden egyes helyzetet összefüggéseiben kell vizsgálni, és az alapján dönthető el az államnak való betudhatóság. Ennek megállapításánál a problémák ott vannak, hogy nagyon nehéz bizonyítani, ugyanis nem elegendő az, hogy egy állam kiberinfrastruktúrájából indult a művelet, még kevésbe az, hogy az állam infrastruktúrát felhasználva magánszemélyek, vagy csoportok állami megbízásból hajtották végre az ártalmas tevékenységet. Az is előfordulhat, hogy a támadók másik államra próbálják terelni a gyanút, így nehéz megbizonyosodni a valódi szereplő(k) kilétéről.[49]

2. IT Army

2022. február 24-én Oroszország megtámadta Ukrajnát, de még ezen lépés előtt is körvonalazódott az ukrán oldalon egy önkéntes kiberhadsereg létrehozására irányuló igény. Az ötletet Yegor Aushev informatikai vállalkozó vetette fel a digitális miniszternek, Mykhailo Federovnak, majd bele is kezdett a vállalkozó

49 Schmitt: i. m. (2017) 111–135.

szellemű résztvevők toborzásába. Az elképzelés egy támadó és egy védekező csoport létrehozása volt. A védekezés az infrastruktúrákra fog irányulni, az agresszor csapat pedig kiberkémkedéssel segítené Ukrajnát az oroszokkal szemben. Így jött létre ad hoc jelleggel az IT-hadsereg, anélkül, hogy bármiféle triviális tervük lett volna, végül hibrid konstrukcióvá alakult. Aushev fő célja az önkéntesek toborzásával a kritikus infrastruktúrák megvédése. A csatlakozók a védelmi minisztérium megbízásából elektronikus kémkedési műveleteket folytatnak,[50] a minisztérium az együttműködésüket azonban nem ismerte el.[51] 2022. február 26-án az ukrán miniszterelnök- helyettes felhívta az informatikai hadsereget, az orosz kormányzati, banki és vállalati weboldalak elérhetetlenné tételére.[52] Készült egy dokumentum, amely konkrét utasításokat tartalmaztak arra vonatkozóan például, hogy milyen szervert használjanak vagy hogyan rejtsék el személyazonosságukat.[53] Az IT-hadsereg két részből áll, az első egy kollektív felhíváshoz kapcsolódik, elsősorban az orosz infrastruktúra elleni összehangolt kiberműveletben való részvételre, amihez bárki csatlakozhat, aki kellő elkötelezettséget érez iránta. A másik belső rész egyre összetettebb támadásokat intéz orosz célpontok ellen. Ez alapján egy ez hierarchikus felépítésű szervezet, ahol laikusok és szakértők (civilek, katonák, hírszerzők) egyaránt közreműködnek a kibertevékenységekben. A hadsereg kormányzati weblapokat és polgári infrastruktúrákat egyaránt célba vesz, a támadások alól online gyógyszertárak, bankok, ételkiszál-

50 Ella-Magdalena Ciuperca – Victor Adrian Vevera: *Solving and managing moral dilemmas. From the cyber battle field to the future of mankind*, Internatinal Conference RCIC'22, 2020. 136.

51 Anne Sophie Delphin Amdal: *Civilian and Private Actors' Support of Ukrainian National Resistance*, Forsvarets forskningsinstitutt, 2022. 14.

52 Ellen Cornelius: *Anonymous Hacktivism: Flying the Flag of Feminist Ethics for the Ukraine IT Army,* 2022. 2.

53 Ciuperca – Vevera: i. m. 136.

lítási szolgáltatások és még a kiskereskedők sem mentesülnek. Az ukrán kormány hivatalos honlapján megjelent az internetes hadsereg elismerése.[54] A hadsereg által indított támadások nagy része a közigazgatást éri, példaként említve a kormányhivatalokat és a törvényhozó szerveket.[55] 2022. április 6.-án egy videót tettek közzé, amelyben egy orosz katona családját telefonhívásban fenyegették azzal, hogy mindent tudnak róluk, és a katona által elkövetett minden pusztításért felelőssé teszik majd őket. Federovnak két díjat ítéltek Lengyelországban az ellenállás megszervezéséért, amiről úgy nyilatkozott, hogy ez a kiberháborúban részt vett kiberközösség érdeme.[56] Az IT Army weboldalán lehetőség van a hadsereghez csatlakozni, ehhez mindösszesen két lépést kell teljesíteni. Első lépésként egy szoftvert kell telepíteni, a második lépés pedig a támadás indítása. Ezen felül ugyanezen weblapon akár célpontot is lehet javasolni.[57]

Az IT Army tekintetében bizonyosan kimondható, hogy ez hadsereg nem állami szerv, és nem is gyakorolnak állami jogköröket. A szakértők azonban a Tallinn 2.0. kommentárjában rögzítik, hogy ha az állam nem képes egyes feladatait ellátni, a feladatokat rábízhatja magán, vagy önkéntes szervezetekre, és ilyenkor ugyanúgy az állam tehető felelőssé. Erre vonatkozó kommentár viszont nincs az Államfelelősségi Tervezetben. Véleményem szerint ebbe a kategóriába a kézikönyv alapján akár be is lehetne sorolni az IT Army-t, ha valóban önkéntes szervezetről lenne szó, bár ugye itt felvetődik az a probléma, hogy a kormányzat támogatta a csoport létrehozását, és megszabta

54 Stefan Soesanto: „The IT Army of Ukraine: Structure, Tasking, and Eco-System", *CSS Cyberdefense Reports*, Zürich, 2022. 4–7.

55 William D. Done: The Information Technology Army of Ukraine and Cyber Warfare Doctrine, *Journal of Strategic Security*, 2023. 16.4: 2.

56 Soesanto: i. m. 20.

57 IT Army hivatalos weboldala. (https://itarmy.com.ua/).

a felépítését, úgyhogy az önkéntesség ebben a kontextusban némiképp vitatható. Az pedig nem jelenthető ki egyértelműen, hogy a kormányzattól származna az irányítás, utasítás vagy az ellenőrzés, de ha így lenne akkor a hackerek akciói megfeleltethetők lennének a Tallinn 2.0-ban megfogalmazott 17. szabály (a) pontjának, amely úgy szól, hogy az állam felelősségi körébe tartozik a nem állami szereplők olyan tevékenysége, amelyet állami irányítás, utasítás, vagy ellenőrzés alatt követtek el.[58] Ezt az Államfelelősségi Tervet 59. cikke is tartalmazza[59], így ha erre esetlegesen hivatkozni lehetne a Nemzetközi Bíróság előtt. A kézikönyv hiányossága, hogy nem állapít meg különböző betudhatósági szinteket. Az Atlanti Tanács Cyber Statecraft Initiative (az univerzális kihívások kezelésének központi szereplője) igazgatója, Jason Healey tíz felelősségi spektrumot állapított meg, amely azt a célt szolgálja, hogy a felelősség pontosabb meghatározását elősegítse. (1) Államilag tiltott: A kormány segít a harmadik fél támadásának megállításában. (2) Államilag tiltott, de ne megfelelő: A kormány kész lenne együttműködni, csak képtelen megállítani a támadást. (3) Állam által figyelmen kívül hagyott: A kormány tudatában van harmadik felek támadásainak, de politikai okok miatt nem intézkedik. (4) Állami bátorítás: Az ellenőrzést harmadik felek végzik, de a kormány ösztönzi őket. (5) Államilag formált: Az ellenőrzést harmadik felek végzik, de a kormány támogatást nyújt. (6) Államilag koordinált: A kormány irányítja a harmadik fél támadókat azáltal, hogy meghatároznak egy célcsoportot, vagy valamilyen részletet. (7) Állami megrendelés: Az állam harmadik felek meghatalmazottait kérik fel, hogy a nevében támadjanak. (8) Állami bűnözök által irányított: A támadást a kiberhadsereg nem ellenőrzött elemei valósítják meg. (9) Államilag végrehajtott: A támadáshoz a kormány

58 Schmitt: i. m. (2017) 94.

59 *Draft articles on the responsibility of international organizations.*

kiberhadseregét használja fel, akik közvetlen irányítás alatt vannak. (10) Államilag integrált: A kormány hadseregeibe harmadik fél támadóit integrálja.[60] Úgy vélem ebben a körben az ukrán kormányzat felelőssége a 6-os pontba mindenképpen beilleszthető, hiszen egyes részletszabályt lefektetnek az általuk kiadott dokumentumban, és ilyen tekintetben megvalósul az irányítás. A 9-es pontot fogalmazza meg lényegében a Tallinn 2.0. 17. szabálya (a) pontja is (amelyet az Államfelelősségi Tervezet is tartalmaz), de teljes bizonyossággal nem állapítható meg az irányítás, felügyelet vagy ellenőrzés, ahogy arra már fentebb hivatkoztam is. Ha nem lehet alkalmazni a betudhatósági szabályokat, de az állam, vagy a hackercsoport primer normát sért, akkor erre hivatkozva a sértett fél eljárást indíthat.

Az 1977-es Genfi Egyezmény az áldozatok védelméről szóló kiegészítő jegyzőkönyv védelmet biztosít a polgári lakosságnak, és a harci cselekményeket csak a katonai célpontok ellen engedélyezi.[61] Nos, a fentebb említett katona családjának fenyegetése egyértelműen ezzel szembe megy, ugyanis ha a család tagjai, akik civilek, kibertámadás áldozataivá válnak, akkor a kiberharccsoport súlyos jogsértést követne el, és ha esetlegesen Ukrajna betudhatósága megállapítható lenne, akkor az ő tevékenységének minősülne.

A felelős személyeket egyébként, ha más módon nem is, de négy esetkörben egyéni felelősség terheli a Nemzetközi Bíróság Büntető Statútuma szerint, ezek a következők: népirtás, háborús bűncselekmények, emberiesség elleni bűncselekmények és

60 Jason Healey: *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*, The Atlantic Council of the United States, Washington DC, 2001. 2.

61 Magyarországon kihirdetett: 1989. évi 20. törvényerejű rendelet a háború áldozatainak védelmére vonatkozóan Genfben 1949. augusztus 12-én kötött Egyezmények I. és II. kiegészítő Jegyzőkönyvének kihirdetéséről.

agresszió. Ezek leginkább csak a fizikai térben alkalmazhatók, de nem kizárt, hogy egyes pontjai a kibertérben is megvalósuljanak, bár az erre vonatkozó felróhatósági vizsgálat elég szigorú. Fontos, hogy ez nem az állam felelősségét, hanem egyéni felelősséget eredményez.[62]

Konklúzió

Az államok betudhatóságára vonatkozó részletes szabályozás sokáig váratott magára, ugyanis csak a 21. század elején került sor az Államfelelősségi Tervezetben az egyes alapeseteinek átfogó kidolgozására. Előtte, a kevéssé korlátozott államközi erőszakalkalmazás korában aligha találunk erre vonatkozó törekvéseket. Azonban ahogy az erőszak egyes korlátai megfogalmazásra kerültek, és fontossá vált az állam felelősségre vonása, a betudhatóság tisztázására is szükség volt. Az Államfelelősségi Tervezet nyolc alappillért állapított meg, amely megalapozza a betudhatóságot. Bár az ENSZ Közgyűlés által elfogadott határozat nem rendelkezik kötelező erővel, ennek ellenére számtalan ügyben hivatkoztak a bíróságok az államfelelősség valamely esetére, emiatt szokásjogi szabályként felfogható.

Tekintettel arra, hogy a kibertér a hadviselés egy új dimenzióját nyitotta meg, és nagy számmal használták fel az államok támadásaik során, szükség volt a nemzetközi szabályozásban is nyomon követni az eseményeket. Már a 20. század végén is alkalmazták ezt a mechanikát, amikor a NATO honlapját tették ki támadásnak. Az elkövetőket ebben az esetben meg tudták állapítani. Az észt és a grúz támadások során ugyan Oroszországot

62 T/4490. számú törvényjavaslat az Egyesült Nemzetek Diplomáciai Konferenciája által, a Nemzetközi Büntetőbíróság Rómában, 1998. július 17-én elfogadott Statútumának kihirdetéséről.

vádolták, de ennek bizonyítása nem volt kellően megalapozott. Az egyes csúcstalálkozókon a kibervédelmi stratégiákat dolgozták ki, és azokat fejlesztették tovább, ehhez különböző szervezeteket (például Kibervédelmi Kiválósági Központ) hoztak létre. Mivel a kibertér más sajátosságokkal rendelkezik, mint a valós front, ezért az erre mérvadó betudhatósági körök kialakítása is szükségesnek bizonyult. Ezek elsősorban a 2013-mas Tallinni Kézikönyvben fogalmazódtak meg, amely a kiberháborúban alkalmazandó nemzetközi jogról rendelkezik. Az ebben foglaltakat vette át gyakorlatilag a 2017-ben kiadott Tallinn 2.0., csak sokkal részletesebben, betudhatósági kiegészítésekkel, amely a kiberműveletekkel foglalkozik, és lényegében a cselekmények államnak való tulajdonításában nem tértek el az Államfelelősségi Tervezettől, arra támaszkodtak a szakértők a munka megalkotása során. Jelenleg a Tallinn 2.0. az utolsó, amely az államok felelősségével foglalkozik. Ami újdonság, hogy a kommentárban sokkal részletesebben tárgyalja az egyes alapeseteket, amivel jobban elősegíti a betudhatóság megállapítását. Ezt főleg annál a szabálynál értem, ahol a kézikönyv tartalmazza azon önkéntes szervezetek tevékenységét, akik azért látnak el egyes feladatokat, mert az állam erre nem képes, de ettől függetlenül az állami tevékenységnek minősül. Ezt a Tervezet konkrétan nem tartalmazza, pedig ez problémát vethet fel például az ukrán internetes hadseregnél is, mert ha csak annyit fogadunk el, hogy valóban önkéntes szervezetről van szó, akkor erre vonatkozó iránymutatás a Tervezetből nem olvasható ki, ergo szigorúan véve erre nagyon nem lehetne hivatkozni. Ami pedig a kézikönyv hiányossága a korábbi munkához képest, hogy amikor az átengedett szervekről szól, a személyeket nem említi, tehát egy átengedett személy tekintetében nem rendezi a betudhatóságot, továbbá hallgat a kormányra került felkelők és az államot alapító mozgalmak tevékenységeiről. Egyik dokumentum sem szól azokról az állami szervekről, amelyek nem rendelkeznek közhatalmi jogosítvá-

nyokkal, ebből következően az ő tevékenységük nem róható fel az államnak.

Az említett dokumentumok egyike sem bír kötelező erővel, hanem különböző állásfoglalásokat, javaslatokat tartalmaz, de ahogy már utaltam rá, az kijelenthető, hogy a 2001-es ajánlásban szereplő betudhatósági csoportok szokásjogilag rögzülhettek, hiszen arra többször is hivatkoztak. A kibertérben bekövetkező műveletek esetében nem az a releváns, hogy melyik állam területéről indították, hanem melyik állam áll az akció mögött, hiszen a kibertér lehetővé teszi, hogy más államok szervereit, számítógépeit felhasználva tanúsítanak jogellenes magatartást.

Ugyan a felelősségre vonás technikai potenciálja a korábbiakhoz képest jelentősen javultak, de még így is legtöbbször bonyolult, költséges, és rengeteg időt igényel a valós tettes beazonosítása, így a betudhatóság nehezen nyer meghatározást, ugyanis a kibertérben legtöbbször nem marad nyom a támadó után, vagy éppen hamisítással más államok felelősségre vonását kívánja megvalósítani, ezért az egyértelmű bizonyítás nehézségekbe ütközik. Nem beszélve arról, hogy nem nyert megállapítást az a tény, hogy mennyi és milyen bizonyítékot követel meg a betudhatóság megállapítása.[63] Ez azért is komplikációt jelent, mert ha egy védekező állam rosszul méri fel a helyzetet, és hibás érvekre alapozva tesz ellenintézkedést, az szintén nemzetközi jogellenességet eredményez. Ha viszont túl sokat vár az ellenintézkedés megtételével azért, hogy elegendő bizonyítékot gyűjtsön a támadó államnak való tulajdonítás megalapozásáért, és a támadás megszűntével kezdi el cselekményeit, a jogellenesség a védekező állam részéről szintén beáll. Nem beszélve arról, hogy ellenintézkedés megtétele előtt fel kell hívni a jogsértő állam figyelmét a létrehozott jogellenességről, és csak ezután lehet cselekedni.

63 William Banks: Cyber Attribution and State Responsibility, *International Law Studies*, Vol. 97. (2021) No. 43, 1049.

Az ellenintézkedés a másik állam kötelezettségeinek teljesítését szolgálja.[64] A szükségesség és arányosság követelménye, valamint a határidő meggátolja, hogy ezek az ellenintézkedések represszáliába, vagy büntetésbe menjenek át.

A kibertámadások rendkívül sokszínűek lehetnek, így irányulhatnak például weblapok megrongálására, bankrendszer megbénítására, kritikus infrastruktúra támadására, vagy akár szociális intézmények rendszereinek befagyasztására. Elengedhetetlen lenne a támadó azonosítása, hogy az országok és a nemzetközi szervezetek képesek legyenek reagálni. Ennek hiánya zűrzavart és további támadásokat von maga után. Véleményem szerint fontos lenne egy egységes felelősségre vonási szabályozás kidolgozása, ugyanis a Tallinn 2.0. e tekintetben hallgat, ami ahhoz vezethet, hogy mivel az államok betudhatósága esetére nem határoz meg szankciókat, így azok továbbra is folytatják a kibertevékenységeiket mindenféle hátrány bekövetkezése nélkül. Tehát egy olyan rendszer kimunkálása lenne szükséges, amely kellő elrettentést biztosít a kibertérben megvalósuló akcióktól.

Sok szempontban nem született egyetértés, így a bizonyítási szabályokat illetően, a nyilvános felelősségre vonásban és annak következményeiben, aminek az lett az eredménye, hogy a civilek és az ő infrastruktúrájuk ellen irányított kibertámadások szabályai nem kerültek kidolgozásra arra vonatkozóan, hogy mi a helyzet akkor, ha ezeket az erőszak küszöbértéke alatt és fegyveres konfliktuson kívül követik el.[65] Így az államokat semmi nem riasztja vissza attól, hogy további kiberműveleteket hajtsanak végre, mert semmilyen következményekkel nem jár a tettük.

Összességében úgy értékelem a kiberműveletekre vonatkozó betudhatósági szabályokat, hogy maguk a jelenleg érvényes esetkörök kellően kimerítőek, ezért ha ebből nemzetközi jogszabály

64 Schmitt: i. m. (2017)
65 Banks: i. m. 1046–1047.

válna, vagy legalább szokásjogi úton elfogadásra kerülne, akkor az államoknak lehetőségük lenne erre a dokumentumra érdemben hivatkozni. Ehhez azonban egy sokkal átláthatóbb és pontosabb bizonyítási szempontrendszer kidolgozására van szükség. Végső soron az is indokolt volna, hogy a felelősség megállapítása utáni olyan szankciótár kialakítására kerüljön, amely kellő elrettentést nyújt a kibertámadások elkövetésétől, ezáltal a műveletek száma lecsökkenthető lehetne.

A nemzetközi szokásjogban, vagy elismert állami gyakorlatban jelenleg nincs meghatározva, hogy milyen szintű részvétel szükséges ahhoz, hogy az államfelelősség megállapítható legyen a kibertérben, de az idő előrehaladtával a nemzetközi konszenzus alakulhat ki erről.[66] A Cyber Statecraft Initiative által kidolgozott 10-es skála, amely a felelősség egy-egy fokát jelöli meg, jó alap lehet erre. Ez a skála a legpasszívabb felelősségtől a legaktívabb felelősségig jut el attól függően, hogy az állam hogyan viszonyul a támadáshoz.[67]

Magára az Államfelelősségi Tervezetben kimunkált betudhatósági esetkörökre nem kizárt, hogy a Nemzetközi Bíróság figyelembe veszi ítéletében. Probléma viszont, hogy nem léteznek olyan elfogadott és végrehajtható szabályok a beavatkozások államnak való betudhatósága kapcsán, amely az elejétől a végéig rendezi a kérdést. Szükséges lenne a bizonyításra vonatkozó pontos előírások megteremtése, főleg amiatt, mert egy ellenintézkedés nem megfelelő bizonyítékokra alapítása a sértett államnak is felróhatóságot eredményez. Továbbá célszerű lenne egy mindenki számára hozzáférhető nyilvántartás, amellyel esetlegesen vissza lehetne fogni a virtuális támadásokat, és segíthetik a többi államot a védekezésben. Mivel nincs megadva, hogy mi az a minimum részvétel, ami megalapozza az államfelelősséget,

66 Banks: i. m. 1067.
67 Healey: i. m. 2.

segítené a betudhatóság megállapítását az a (vagy ilyen) tízfokozatú spektrum, amit az Atlanti Tanácsban megfogalmaztak a kibertérben megvalósuló akciókra. Mindazonáltal az államok közötti kollektív megállapodás elősegíti a támadók megtalálását, és fejleszti a részes államok kibervédelmét, illetve a felróhatóság hitelességét is igazolja. Törekedni kell az ilyen szerződések létrehozására. Végső soron egy részletes szankciótár kidolgozása is indokolt volna, amely a betudhatóság fokozataira tekintettel pontosan determinálja, hogy milyen következményekkel jár az elkövetett kiberbűncselekmény, amely visszafoghatná a támadókat.

Ha a kibertámadásokban az állam felelőssége nem állapítható meg, valamilyen módon mégiscsak szükséges a bűnösök felelősségre vonása, ezért a primer normasértésekre ettől függetlenül lehet hivatkozni, illetve ha népirtás, háborús deliktum, emberiesség elleni bűncselekmény, vagy agresszió valósul meg, egyéni felelősségre vonásra is van lehetőség,[68] de közel sem biztos, hogy ezek szintjét egy virtuális művelet eléri.

68 T/4490. számú törvényjavaslat.